# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 04-086135

(43)Date of publication of application : 18.03.1992

(51)Int.Cl. H04L 9/06
H04L 9/14

(21)Application number : 02-201722

(22)Date of filing : 30.07.1990

(71)Applicant : SHARP CORP

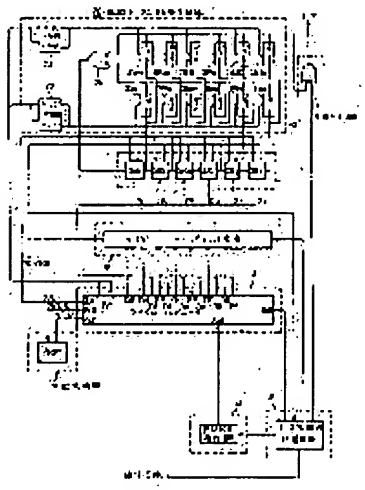
(72)Inventor : HIRAIDE JUNJI
TADA JUNJI

(54) PRIVACY CALL DEVICE

(57)Abstract:

PURPOSE: To enhance the privacy call performance by decoding a data based on the result of decoding of an address data ciphered by a pseudo random signal.

CONSTITUTION: An address data included in a signal from a communication line in the case of reception is fed to a microcomputer 6 via a serial/parallel conversion circuit 10 from a changeover circuit 8. Then the address data is fed to a storage circuit 3 from the microcomputer 6 to read relevant initial value data D1-D6, a stage number setting data and a tap position setting data. A decoding circuit 11 uses a pseudo random signal to decode accurately the ciphered data from the changeover circuit 8 and outputs the resulting data.



Thus, it is not required for the receiver side to enter a signal key, and the sender side revises freely a cryptographic key and the secrecy of the communication is sufficiently kept.

⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　平4−86135

⑤Int. Cl.⁵　識別記号　庁内整理番号　⑬公開　平成4年(1992)3月18日

H 04 L 9/06
9/14

7117−5K　H 04 L 9/02　Z

審査請求　未請求　請求項の数 2　（全12頁）

⑭発明の名称　秘話装置

⑳特　願　平2−201722

㉒出　願　平2(1990)7月30日

⑰発明者　平出　順二　大阪府大阪市阿倍野区長池町22番22号　シャープ株式会社内

⑰発明者　多田　順次　大阪府大阪市阿倍野区長池町22番22号　シャープ株式会社内

⑪出願人　シャープ株式会社　大阪府大阪市阿倍野区長池町22番22号

## 明　細　書

1　発明の名称

秘話装置

2．特許請求の範囲

（1）送信側には、

シフトレジスタを使用して構成される第1の疑似ランダム信号発生回路と、

暗号鍵を設定する暗号鍵設定手段と、

上記第1の疑似ランダム信号発生回路の初期値データ、段数設定データおよびタップ位置設定データ等の初期設定データを記憶した第1の記憶回路と、

上記暗号鍵設定手段からの暗号鍵に対応したアドレスデータによって上記第1の記憶回路から上記初期設定データを読み出して上記第1の疑似ランダム信号発生回路を設定する第1の制御手段と、

上記第1の疑似ランダム信号発生回路の出力信号によって入力データを暗号化する暗号化回路とが備えられ、

上記暗号化回路の出力データおよび上記アドレスデータが送信され、

受信側には、

上記第1の疑似ランダム信号発生回路と同じ構成の第2の疑似ランダム信号発生回路と、

上記第1の記憶回路と同じ内容を記憶した第2の記憶回路と、

受信した上記アドレスデータによって上記第2の記憶回路から上記初期設定データを読み出して上記第2の疑似ランダム信号発生回路を設定する第2の制御手段と、

上記第2の疑似ランダム信号発生回路の出力信号によって受信したデータを復号化する復号化回路とが備えられることを特徴とする秘話装置。

（2）送信側には、

第1の疑似ランダム信号発生回路と、

初期設定データが固定値とされる第2の疑似ランダム信号発生回路と、

暗号鍵を設定する暗号鍵設定手段と、

上記第1の疑似ランダム信号発生回路の初期設

定データを記憶した第１の記憶回路と、

上記暗号設定手段からの暗号鍵に対応したアドレスデータによって上記第１の記憶回路から上記初期設定データを読み出して上記第１の疑似ランダム信号発生回路を設定する第１の制御手段と、

上記第１の疑似ランダム信号発生回路の出力信号によって入力データを暗号化する第１の暗号化回路と、

上記第２の疑似ランダム信号発生回路の出力信号によって上記アドレスデータを暗号化する第２の暗号化回路とが備えられ、

第１および第２の暗号化回路の出力データが送信され、

受信側には、

上記第１および第２の疑似ランダム信号発生回路とそれぞれ同じ構成の第３および第４の疑似ランダム信号発生回路と、

上記第１の記憶回路と同じ内容を記憶した第２の記憶回路と、

上記第４の疑似ランダム信号発生回路によって受信した上記第２の暗号化回路の出力データを復号化する第１の復号化回路と、

上記第１の復号化回路より出力されるアドレスデータによって上記第２の記憶回路から上記初期設定データを読み出して上記第３の疑似ランダム信号発生回路を設定する第２の制御手段と、

上記第３の疑似ランダム信号発生回路の出力信号によって受信した上記第１の暗号化回路の出力データを復号化する第２の復号化回路とが備えられることを特徴とする秘話装置。

## 3．発明の詳細な説明

〔産業上の利用分野〕

この発明は、例えば有線あるいは無線ディジタル通信に使用して好適な秘話装置に関する。

〔従来の技術〕

通信において、通信内容が秘密である場合には秘話通信を行なう必要がある。この場合、送信側では、通常データ（平文）が暗号化され、この暗号化データ（暗号文）が送信される。そして、受信側では、この暗号文が平文に復号化される。

第９図は、従来の秘話装置を示している。

同図において、送信側では、平文が暗号化回路１３に供給されて暗号鍵１５に応じて暗号文に変換される。この暗号化回路１３からの暗号文は、有線または無線の通信区間を介して、受信側に供給される。また、受信側では、暗号文が復号化回路１４に供給されて復号鍵１６に応じて平文に変換される。

〔発明が解決しようとする課題〕

第９図例によれば、送信側および受信側が、暗号化および復号化のために、例えば同一の鍵を所有する必要がある。そのため、送信側では暗号鍵を自由に変更することができなかった。しかし、通信の秘密を確保するには、暗号鍵を度々変更する必要がある。

そこで、本出願人は、先に、暗号鍵を自由に変更できる秘話装置を提案した（特願平１－７０２００号）。以下、この秘話装置について説明する。

第６図は送信側のブロック図である。

同図において、２０は疑似ランダム信号発生回路であり、この疑似ランダム信号発生回路２０は、６段のシフトレジスタＳＲ１～ＳＲ６の縦続接続段１と、この縦続接続段１の帰還路を選択する切り替え回路２とで構成される。

縦続接続段１のシフトレジスタＳＲ１～ＳＲ６のロードおよびシフト状態は、制御手段であるマイクロコンピュータ６からの制御信号Ｓ／Ｌによって制御される。制御信号Ｓ／Ｌがロード状態のとき、シフトレジスタＳＲ１～ＳＲ６には、マイクロコンピュータ６からの初期値データＤ１～Ｄ６がロードされる。なお、これらシフトレジスタＳＲ１～ＳＲ６はクロックＣＫに同期して動作するようにされる。

切り替え回路２は、ゲートおよびインバータで構成される。すなわち、アンドゲート２１にはシフトレジスタＳＲ６の出力信号が供給されると共に、マイクロコンピュータ６からの制御データＤ７が供給される。また、アンドゲート２３にはシフトレジスタＳＲ１の出力信号が供給されると共に、制御

データD7がインバータ22を介して供給される。そして、これらアンドゲート21および23の出力信号がオアゲート24に供給される。したがって、制御データD7がハイレベルかローレベルかに応じて、オアゲート24からはシフトレジスタSR1またはSR5の出力信号が出力される。

また、エクスクルーシブオアゲート25にはオアゲート24の出力信号が供給されると共に、シフトレジスタSR6の出力信号が供給される。そして、このエクスクルーシブオアゲート25の出力信号はシフトレジスタSR1に帰還される。したがって、シフトレジスタSR1～SR6がシフト動作をするとき、シフトレジスタSR6からは初期値データD1～D6および切り替え回路2の選択に応じた疑似ランダム信号が出力される。

また、5は暗号鍵設定手段であり、この暗号鍵設定手段5は、ハイレベルまたはローレベルを選択する7個の接続スイッチで構成される。これら7個の接続スイッチの一端は電源端子に接続され、その他端はマイクロコンピュータ6の端子Pi1～Pi7に接続される。

また、3は例えばROM（リードオンリーメモリ）で構成される記憶回路であり、この記憶回路3には複数段構成1のシフトレジスタSR1～SR6に供給される初期値データD1～D6と、切り替え回路2に供給される制御データD7とが複数組記憶されている。

この場合、暗号鍵設定手段5で設定された暗号鍵に応じたアドレスデータがマイクロコンピュータ6より記憶回路3に供給され、対応する初期値データD1～D6および制御データD7が読み出される。そして、この初期値データD1～D6および制御データD7はマイクロコンピュータ6の端子Po1～Po7を介してシフトレジスタSR1～SR6および切り替え回路2に供給され、これにより疑似ランダム信号発生回路20が初期設定される。

また、マイクロコンピュータ6からのアドレスデータはパラレル／シリアル変換回路4でシリアル信号に変換されて出力される。

また、7はエクスクルーシブオアゲートで構成される暗号化回路であり、この暗号化回路7には、疑似ランダム信号発生回路20からの疑似ランダム信号と、データ発生手段（図示せず）からのシリアルデータ（例えば、音声データ）とが供給されて、シリアルデータは暗号化される。

また、8はデータ／制御信号切り替え回路であり、この切り替え回路8には変換回路4より出力されるアドレスデータ、暗号化回路7より出力される暗号化データおよび同期信号発生回路9からの同期信号が供給される。そして、マイクロコンピュータ6の制御により、これらの信号はクロックCKに同期して切り替えられ、有線または無線の通信回線に出力される。第8図はその通信信号の構成例を示している。

このように、送信側では、暗号鍵設定手段5による暗号鍵の設定に応じて、データが暗号化され、同期信号およびアドレス信号と共に、通信回線に出力される。

第7図は、受信側のブロック図である。この第7図において、第6図と対応する部分には同一符号を付して示している。

同図において、通信回線からの信号はデータ／制御信号切り替え回路8を介して同期信号検出回路12に供給され、この同期信号検出回路12で検出される同期信号（第8図参照）はマイクロコンピュータ6に供給される。

また、切り替え回路8には、マイクロコンピュータ6より同期信号に応じて制御信号およびクロックCKが供給される。そして、通信回線からの信号に含まれるアドレスデータは切り替え回路8よりシリアル／パラレル変換回路10でパラレル信号に変換されたのちマイクロコンピュータ6に供給される。そして、このアドレスデータはマイクロコンピュータ6より記憶回路3に供給され、対応する初期値データD1～D6および制御データD7が読み出される。そして、この初期値データD1～D6および制御データD7はマイクロコンピュータ6の端子Po1～Po7を介して疑似ランダム信号発生回路20のシフトレジスタSR1～SR6および切り替え回路2に供給される。これにより疑似

ランダム信号発生回路２０が初期設定される。

この場合、受信側および送信側の記憶回路３の記憶内容は同じであると共に、受信側および送信側の疑似ランダム信号発生回路２０は同じ構成であるので、受信側の疑似ランダム信号発生回路２０からは、送信側と同様の疑似ランダム信号が発生される。

また、１１はエクスクルーシブオアゲートで構成される復号化回路である。この復号化回路１１には、疑似ランダム信号発生回路２０からの疑似ランダム信号と、切り替え回路８からの暗号化データとが供給され、暗号化データは復号化されて出力される。

このように第６図および第７図に示す秘話装置によれば、受信側で復号鍵を入力する必要はなく、送信側で暗号鍵を自由に変更することができる。

ところで、暗号は前に第５者により解読される危険性を持っており、より秘話性の高い装置が要求される。

そこで、この発明では、秘話性をさらに高めた秘話装置を提供するものである。

〔課題を解決するための手段〕

第１の発明に係る秘話装置は以下のように構成される。

送信側には、シフトレジスタを使用して構成される第１の疑似ランダム信号発生回路と、暗号鍵を設定する暗号鍵設定手段と、第１の疑似ランダム信号発生回路の初期値データ、段数設定データおよびタップ位置設定データ等の初期設定データを記憶した第１の記憶回路と、暗号鍵設定手段からの暗号鍵に対応したアドレスデータによって第１の記憶回路から初期設定データを読み出して第１の疑似ランダム信号発生回路を設定する第１の制御手段と、第１の疑似ランダム信号発生回路の出力信号によって入力データを暗号化する暗号化回路とが備えられ、暗号化回路の出力データおよびアドレスデータが送信される。

受信側には、第１の疑似ランダム信号発生回路と同じ構成の第２の疑似ランダム信号発生回路と、第１の記憶回路と同じ内容を記憶した第２の記憶回路と、受信したアドレスデータによって第２の記憶回路から初期設定データを読み出して第２の疑似ランダム信号発生回路を設定する第２の制御手段と、第２の疑似ランダム信号発生回路の出力信号によって受信したデータを復号化する復号化回路とが備えられる。

第２の発明に係る秘話装置は、以下のように構成される。

送信側には、第１の疑似ランダム信号発生回路と、初期設定データが固定値とされる第２の疑似ランダム信号発生回路と、暗号鍵を設定する暗号鍵設定手段と、第１の疑似ランダム信号発生回路の初期設定データを記憶した第１の記憶回路と、暗号設定手段からの暗号鍵に対応したアドレスデータによって第１の記憶回路から初期設定データを読み出して第１の疑似ランダム信号発生回路を設定する第１の制御手段と、第１の疑似ランダム信号発生回路の出力信号によって入力データを暗号化する第１の暗号化回路と、第２の疑似ランダム信号発生回路の出力信号によってアドレスデータを暗号化する第２の暗号化回路とが備えられ、第１および第２の暗号化回路の出力データが送信される。

受信側には、第１および第２の疑似ランダム信号発生回路とそれぞれ同じ構成の第３および第４の疑似ランダム信号発生回路と、第１の記憶回路と同じ内容を記憶した第２の記憶回路と、第４の疑似ランダム信号発生回路によって受信した第２の暗号化回路の出力データを復号化する第１の復号化回路と、第１の復号化回路より出力されるアドレスデータによって第２の記憶回路から初期設定データを読み出して第３の疑似ランダム信号発生回路を設定する第２の制御手段と、第３の疑似ランダム信号発生回路の出力信号によって受信した第１の暗号化回路の出力データを復号化する第２の復号化回路とが備えられる。

〔作　用〕

第１の発明においては、疑似ランダム信号発生回路の段数、タップ位置を自由に設定することができ、秘話性をより高めることが可能となる。

第２の発明においては、アドレスデータが疑似ランダム信号によって暗号化され、このアドレスデータの復号結果に基づいて、データの復号化が行なわれるので、秘匿性をより高めることができる。

【実施例】

以下、図面を参照しながら、第１の発明の一実施例について説明する。

第１図は、送信側のブロック図である。この第１図において、第６図と対応する部分には同一符号を付し、その詳細説明は省略する。

本例においては、暗号鍵設定手段５からの信号鍵は演算回路で構成される暗号鍵変換回路１７を介してマイクロコンピュータ６に供給される。変換回路１７にはマイクロコンピュータ６より通信回数のデータが供給され、暗号鍵設定手段５より供給される暗号鍵は通信ごとに異なるように変更される。

このように変更するための演算処理例としては、通信ごとに「１」を加算していくというような簡単なものから、ＰＮ発生回路によるスクランブル化、乗算、除算等各種演算による複雑なものまで考えられる。

また本例において、疑似ランダム信号発生回路２０は、６段のシフトレジスタＳＲ１～ＳＲ６の縦続接続段１と、使用するシフトレジスタの段数および帰還のためのタップ位置を切り替える切り替え回路２′とで構成され、シフトレジスタＳＲ１～ＳＲ６のロードおよびシフト状態は、第６図例と同様に、マイクロコンピュータ６からの制御信号Ｓ／Ｌによって制御される。

シフトレジスタＳＲ１～ＳＲ６の出力信号は、それぞれ接続スイッチＳＷ１１～ＳＷ１６を介してエクスクルーシブオアゲート２６に供給されると共に、それぞれ接続スイッチＳＷ２１～ＳＷ２６を介してエクスクルーシブオアゲート２６および暗号化回路７に供給される。そして、エクスクルーシブオアゲート２６の出力信号は、シフトレジスタＳＲ１に供給される。

接続スイッチＳＷ１１～ＳＷ１６のオンオフは、それぞれクップ切り替え用デコーダ２７の出力信号によって制御される。つまり、いずれか１つがオンとされ、帰還のためのタップ位置が設定される。

接続スイッチＳＷ２１～ＳＷ２６のオンオフは、それぞれ段数切り替え用デコーダ２８の出力信号によって制御される。つまり、いずれか１つがオンとされ、使用されるシフトレジスタの段数が設定される。

また本例において、記憶回路３には、縦続接続段１のシフトレジスタＳＲ１～ＳＲ６に供給される初期値データＤ１～Ｄ６、段数切り替え用デコーダ２８に供給される段数設定データおよびタップ切り替え用デコーダ２７に供給されるタップ位置設定データが複数組記憶されている。

以上の構成において、送信をする際には、変換回路１７でもって変更された暗号鍵に応じたアドレスデータがマイクロコンピュータ６より記憶回路３に供給され、対応する初期値データＤｉ～Ｄ６、段数設定データおよびタップ位置設定データが読み出される。

そして、初期値データＤ１～Ｄ６はマイクロコンピュータ６の端子Ｐ０１～Ｐ０６を介してシフトレジスタＳＲ１～ＳＲ６に供給され、この初期値データＤ１～Ｄ６がシフトレジスタＳＲ１～ＳＲ６にロードされて、初期値がセットされる。

段数設定データはマイクロコンピュータ６の端子Ｐ０７を介して段数切り替え用デコーダ２８に供給され、このデコーダ２８からは段数設定データに対応した信号が出力され、これにより接続スイッチＳＷ２１～ＳＷ２６のオンオフが制御されて、段数が設定される。

タップ位置設定データはマイクロコンピュータ６の端子Ｐ０７を介してタップ切り替え用デコーダ２７に供給され、このデコーダ２７からはタップ位置設定データに対応した信号が出力され、これにより接続スイッチＳＷ１１～ＳＷ１６のオンオフが制御されて、タップ位置が設定される。

その結果、疑似ランダム信号発生回路２０からは、シフトレジスタＳＲ１～ＳＲ６にセットされた初期値、設定された段数および設定されたタップ

位置に応じた疑似ランダム信号が出力され、暗号化回路7では、この疑似ランダム信号でもってデータが暗号化される。

なお、その他の部分に関しては、第6図例と同様であり、説明は省略する。

次に、第2図は、受信側のブロック図である。この第2図において、第7図と対応する部分には同一符号を付し、その詳細説明は省略する。

本例において、疑似ランダム信号発生回路20および記憶回路3は、第1図の送信側と同様に構成される。

以上の構成において、受信をする際、通信回線からの信号に含まれるアドレスデータは、切り替え回路8よりシリアル/パラレル変換回路10を介してマイクロコンピュータ6に供給される。そして、このアドレスデータは、マイクロコンピュータらより記憶回路3に供給され、対応する初期値データD1～D6、段数設定データおよびタップ位置設定データが読み出される。

そして、初期値データD1～D6はマイクロコンピュータ6の端子P01～P06を介してシフトレジスタSR1～SR6に供給され、この初期値データD1～D6がシフトレジスタSR1～SR6にロードされて、初期値がセットされる。

段数設定データはマイクロコンピュータ6の端子P07を介して段数切り替え用デコーダ28に供給され、このデコーダ28からは段数設定データに対応した信号が出力され、これにより接続スイッチSW21～SW26のオンオフが制御されて、段数が設定される。

タップ位置設定データはマイクロコンピュータ6の端子P07を介してタップ切り替え用デコーダ27に供給され、このデコーダ27からはタップ位置設定データに対応した信号が出力され、これにより接続スイッチSW11～SW16のオンオフが制御されて、タップ位置が設定される。

この場合、受信側および送信側の記憶回路3の記憶内容は同じであると共に、受信側および送信側の疑似ランダム信号発生回路20は同じ構成であるので、疑似ランダム信号発生回路20は送信側と同様に設定され、送信側と同様の疑似ランダム信号が発生される。

そのため、復号化回路11では、この疑似ランダム信号でもって切り替え回路8からの暗号化データが正確に復号化され、データが出力される。

なお、その他の部分に関しては、第7図例と同様であり、説明は省略する。

このように第1図および第2図に示す秘話装置によれば、受信側で復号鍵を入力する必要はなく、送信側で暗号鍵を自由に変更することができる。

また、暗号鍵に応じて疑似ランダム信号発生回路20の初期値だけでなく、ハード構成（段数、タップ位置）も変更されるので、秘話性を高めることができる。

さらに、暗号鍵は変換回路17で通信毎に異なるように変更されるので、ユーザーを煩わせることなく、通信の秘話を充分に保持することができる。

次に、第2の発明の一実施例について説明する。

第3図は、送信側のブロック図である。この第3図において、第6図と対応する部分には同一符号を付し、その詳細説明は省略する。

本例において、暗号鍵設定手段5からの暗号鍵は演算回路で構成される暗号鍵変換回路17を介してマイクロコンピュータ6に供給される。変換回路17にはマイクロコンピュータ6より通信回数のデータが供給され、暗号鍵設定手段5より供給される暗号鍵は通信ごとに異なるように変更される。

このように変更するための演算処理例としては、通信ごとに「1」を加算していくというような簡単なものから、PN発生回路によるスクランブル化、乗算、除算やそ種演算による複雑なものまで考えられる。

また、本例においては、疑似ランダム信号発生回路20の他に、同様の構成とされた疑似ランダム信号発生回路20'が設けられる。縦続接続段1のシフトレジスタSR1～SR6のロードおよびシフト状態は、マイクロコンピュータ6からの制御信号S/Lによって制御される。

また、この疑似ランダム信号発生回路２０′の初期設定は、マイクロコンピュータ６の端子Ｐｏ１～Ｐｏ６より複数接続段１のシフトレジスタＳＲ１～ＳＲ６に初期値データＤ１′～Ｄ６′が供給されてセットされると共に、マイクロコンピュータ６の端子Ｐｏ７より切り替え回路２に制御データＤ７′が供給されて増巾のためのタップ位置が設定される。この場合、初期値データＤ１′～Ｄ６′、制御データＤ７′は固定値とされる。

疑似ランダム信号発生回路２０′からの疑似ランダム信号は、エクスクルーシブオアゲートで構成される暗号化回路７′に供給される。この暗号化回路７′には、パラレル／シリアル変換回路４でシリアルデータとされたアドレスデータが供給され、疑似ランダム信号でもって暗号化される。そして、この暗号化回路７′からの暗号化されたアドレスデータはデータ／制御信号切り替え回路８に供給される。

以上の構成において、送信をする際には、変換回路１７でもって変更された暗号鍵に応じたアドレスデータがマイクロコンピュータ６より記憶回路３に供給され、対応する初期値データＤ１～Ｄ６および制御データＤ７が読み出される。そして、この初期値データＤ１～Ｄ６および制御データＤ７は、マイクロコンピュータ６の端子Ｐｏ１～Ｐｏ７を介して疑似ランダム信号発生回路２０のシフトレジスタＳＲ１～ＳＲ６および切り替え回路２に供給され、これにより疑似ランダム信号発生回路２０が初期設定される。

その結果、疑似ランダム信号発生回路２０からは、シフトレジスタＳＲ１～ＳＲ６にセットされた初期値、切り替え回路２で設定されたタップ位置に応じた疑似ランダム信号が出力され、暗号化回路７では、この疑似ランダム信号でもってデータが暗号化され、この暗号化データは切り替え回路８に供給される。

また、固定値である初期値データＤ１′～Ｄ６′および制御データＤ７′がマイクロコンピュータ６の端子Ｐｏ１～Ｐｏ７を介して疑似ランダム信号発生回路２０′のシフトレジスタＳＲ１～ＳＲ６および切り替え回路２に供給され、これにより疑似ランダム信号発生回路２０′が初期設定される。

その結果、疑似ランダム信号発生回路２０からは、シフトレジスタＳＲ１～ＳＲ６にセットされた初期値、切り替え回路２で設定されたタップ位置に応じた疑似ランダム信号が出力され、暗号化回路７′では、この疑似ランダム信号でもってアドレスデータが暗号化され、この暗号化されたアドレスデータは切り替え回路８に供給される。

したがって、切り替え回路８から通信回線には、第５図に示すような通信信号が出力される。

なお、その他の部分に関しては、第６図例と同様であり、説明は省略する。

次に、第４図は、受信側のブロック図である。この第４図において、第７図と対応する部分には同一符号を付し、その詳細説明は省略する。

本例においては、送信側と同様の構成の疑似ランダム信号発生回路２０′が設けられる。複数接続段１のシフトレジスタＳＲ１～ＳＲ６のロードおよびシフト状態は、マイクロコンピュータ６からの制御信号Ｓ／Ｌによって制御される。この疑似ランダム信号発生回路２０′の初期設定は、固定の初期値データＤ１′～Ｄ６′および制御データＤ７′がマイクロコンピュータ６の端子Ｐｏ１～Ｐｏ７よりシフトレジスタＳＲ１～ＳＲ６および切り替え回路２に供給されて行なわれる。

疑似ランダム信号発生回路２０′からの疑似ランダム信号は、エクスクルーシブオアゲートで構成される復号化回路１１′に供給される。この復号化回路１１′には、切り替え回路８より暗号化されたアドレスデータが供給される。そして、復号化回路１１′の出力信号は、シリアル／パラレル変換回路１０に供給される。

以上の構成において、受信をする際には、通信回線からの信号に含まれる同期信号に基づいて、マイクロコンピュータ６の端子Ｐｏ１～Ｐｏ７の端子より疑似ランダム信号発生回路２０′に初期値データＤ１′～Ｄ６′および制御データＤ７′が供給されて初期設定される。

そして、通信回線からの信号に含まれる暗号化

されたアドレスデータは、切り替え回路８より復号化回路１１'に供給されて、疑似ランダム信号発生回路２０'からの疑似ランダム信号でもって復号化される。

この場合、受信側および送信側の疑似ランダム信号発生回路２０'は同じ構成であり、固定の初期値データＤ1'～Ｄ6'および制御データＤ7'で初期設定されるので、受信側の疑似ランダム信号発生回路２０'からは送信側と同様の疑似ランダム信号が発生される。そのため、復号化回路１１'では正確に復号化され、アドレスデータが出力される。

復号化回路１１'からのアドレスデータは、シリアル／パラレル変換回路１０を介してマイクロコンピュータ６に供給される。そして、このアドレスデータは、マイクロコンピュータ６より記憶回路３に供給され、対応する初期値データＤ1～Ｄ6および制御データＤ7が読み出され、マイクロコンピュータ６の端子Ｐ01～Ｐ07を介して疑似ランダム信号発生回路２０に供給されて初期設定される。

そして、通信回線からの信号に含まれる暗号化データは切り替え回路８より復号化回路１１に供給されて、疑似ランダム信号発生回路２０からの疑似ランダム信号でもって復号化される。

この場合、受信側および送信側の記憶回路３の記憶内容は同じであると共に、受信側および送信側の疑似ランダム信号発生回路２０は同じ構成であるので、疑似ランダム信号発生回路２０は送信側と同様に初期設定され、送信側と同様の疑似ランダム信号が発生される。そのため、復号化回路１１では正確に復号化され、データが出力される。

なお、その他の部分に関しては、第７図例と同様であり、説明は省略する。

このように第３図および第４図に示す秘話装置によれば、受信側で復号鍵を入力する必要はなく、送信側で暗号鍵を自由に変更することができる。

また、アドレスデータも暗号化されて送信されるので、受信側ではその復号化が必要となり、秘話性を高めることができる。

さらに、暗号鍵は変換回路１７で通信毎に異なるように変更されるので、ユーザーを煩わせることなく、通信の秘密を充分に保持することができる。

なお、上述実施例においては、疑似信号回路１のシフトレジスタの段数は６段とされたものであるが任意の段数とすることができる。

また、第３図例および第４図例においては、疑似ランダム信号発生回路２０および２０'は同様の構成とされたものであるが、異なる構成としてもよい。

〔発明の効果〕

以上説明したように、第１の発明によれば、受信側で復号鍵を入力する必要はなく、送信側で暗号鍵を自由に変更することができると共に、暗号鍵に応じて疑似ランダム信号発生回路２０の初期値だけでなく、ハード構成（段数、タップ位置）も変更されるので、通信の秘密を充分に保持することができる。

また、第２の発明によれば、受信側で復号鍵を入力する必要はなく、送信側で暗号鍵を自由に変更できると共に、アドレスデータも暗号化されて送信されるので、受信側ではその復号化が必要となり、通信の秘密を充分に保持することができる。

4．図面の簡単な説明

第１図および第２図は第１の発明の一実施例を示すブロック図、第３図および第４図は第２の発明の一実施例を示すブロック図、第５図はその通信信号の構成を示す図、第６図は秘話装置の送信側のブロック図、第７図は秘話装置の受信側のブロック図、第８図は通信信号の構成を示す図、第９図は従来の秘話装置のブロック図である。

３・・・記憶回路
４・・・パラレル／シリアル変換回路
５・・・暗号鍵設定手段
６・・・マイクロコンピュータ
7、7'・・・暗号化回路
８・・・データ／制御信号切り替え回路

9　・・・同期信号発生回路

10・・・シリアル／パラレル変換回路

11、11'

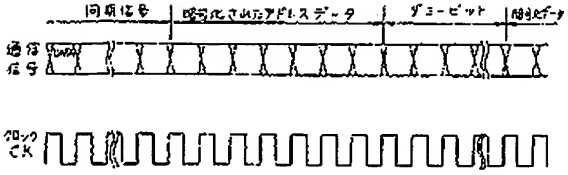
・・・復号化回路

12・・・同期信号検出回路

17・・・暗号鍵変換回路

20、20'

・・・疑似ランダム信号発生回路

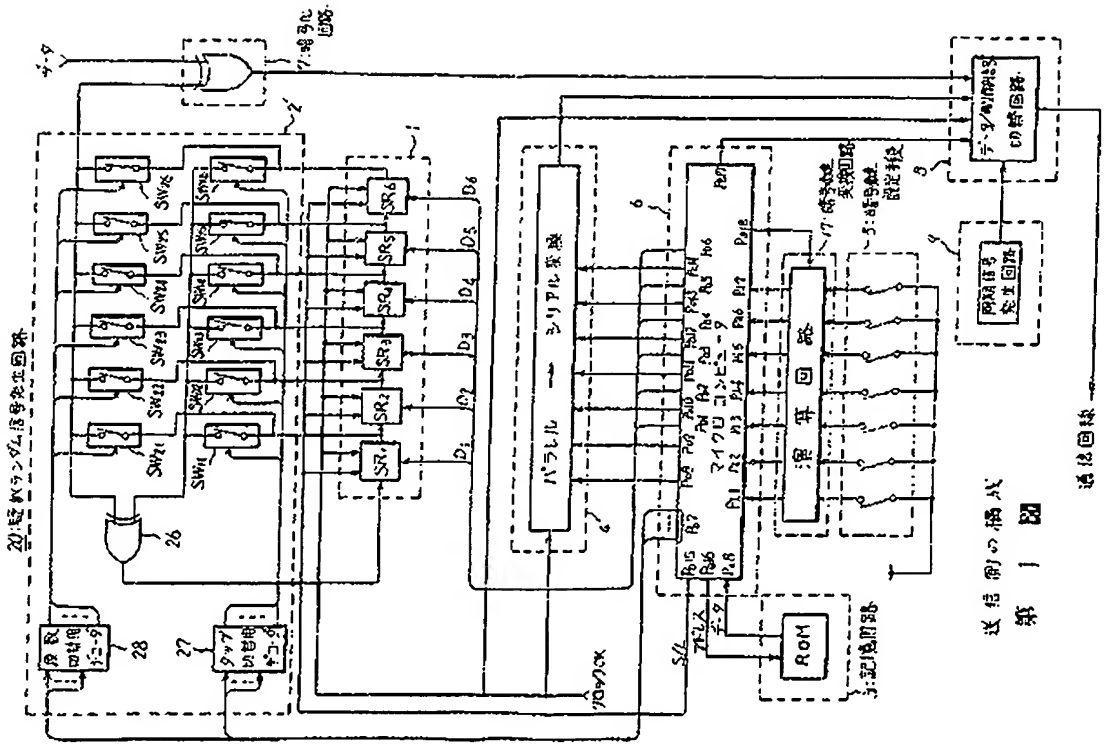



通信信号の一例

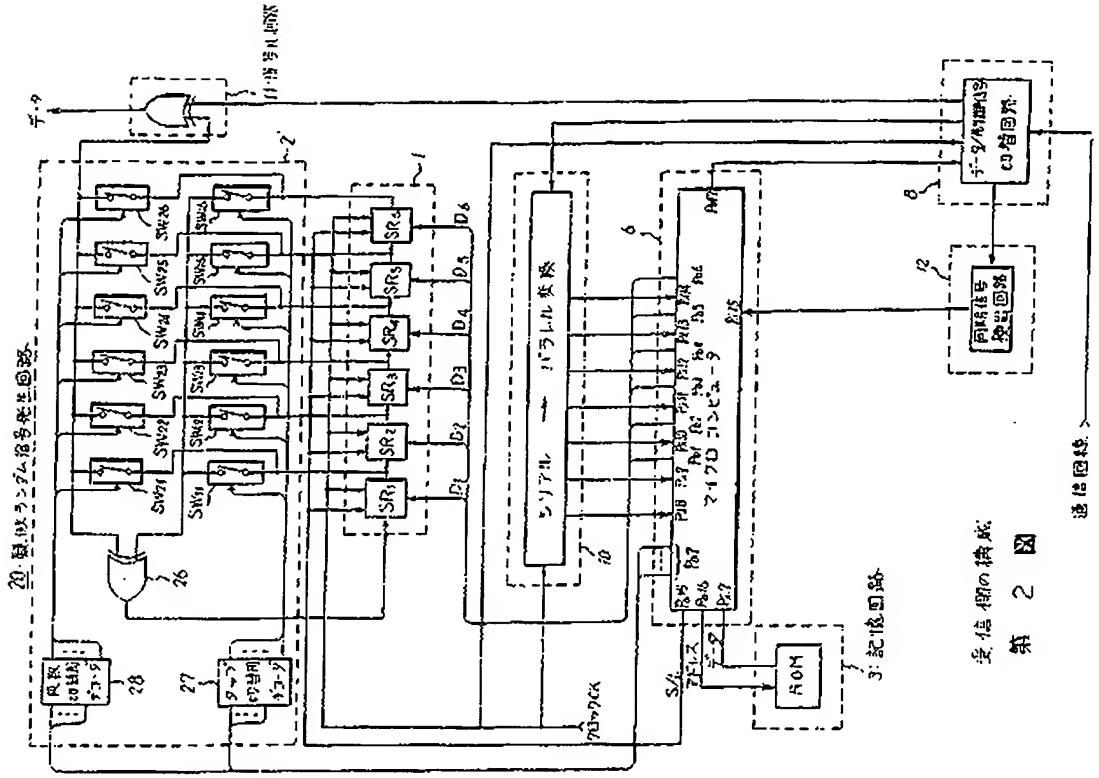
第 5 図

特許出願人　シャープ株式会社

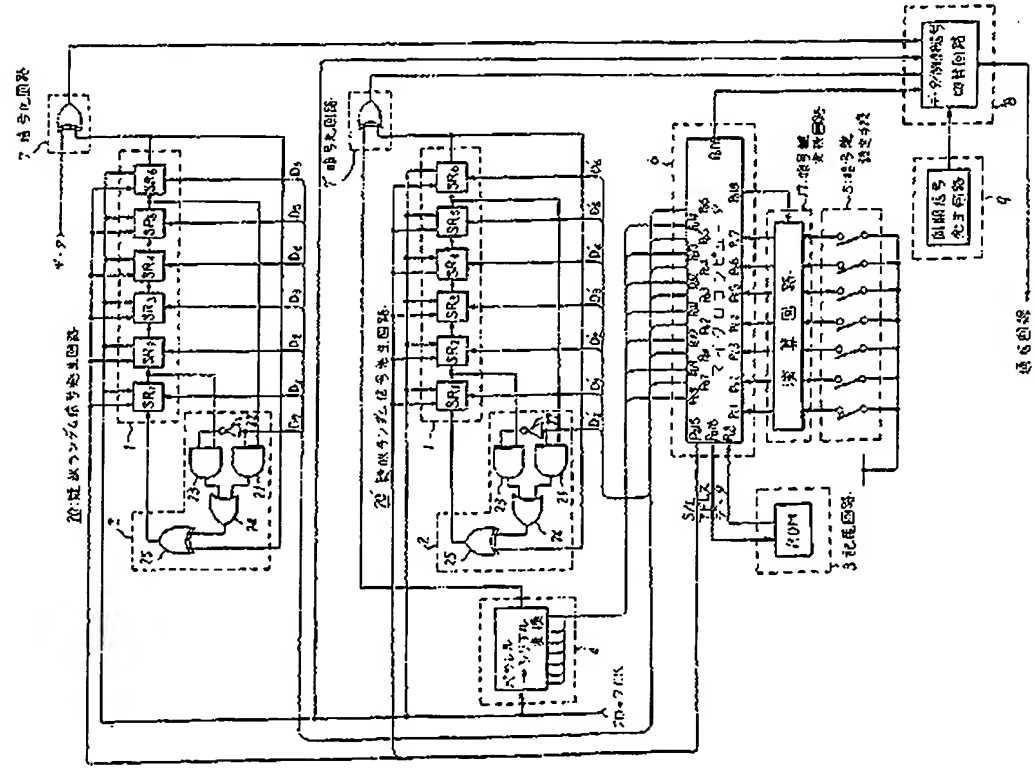
代 理 人　弁理士 山口 邦夫



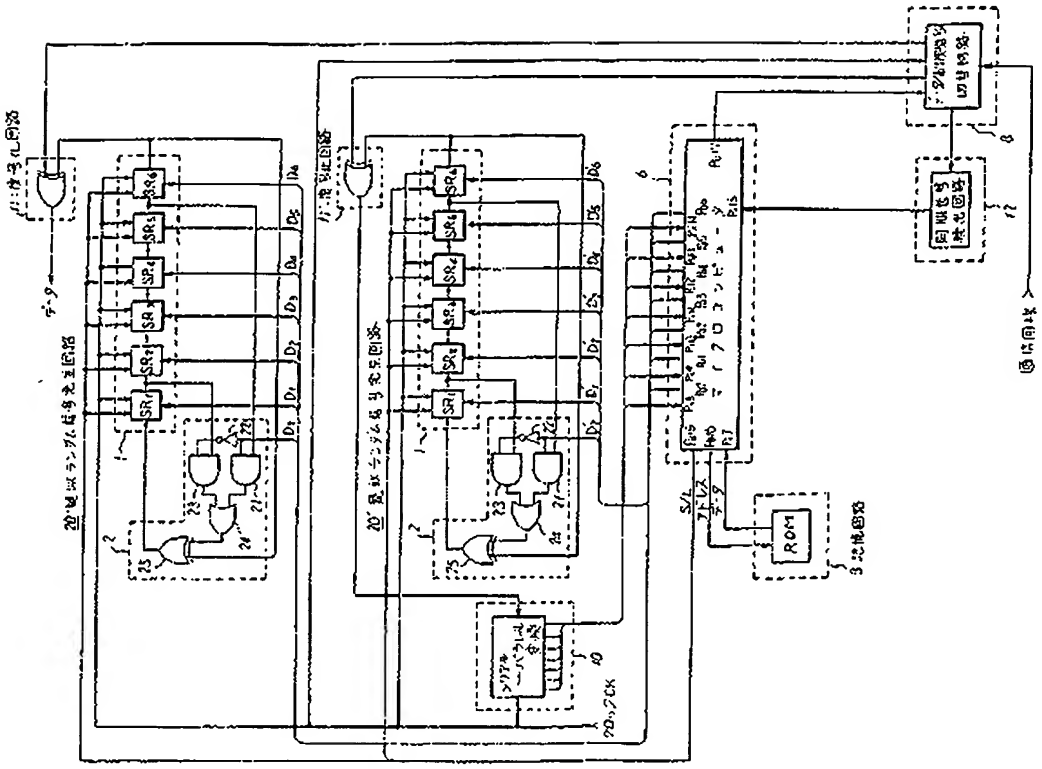

第 1 図



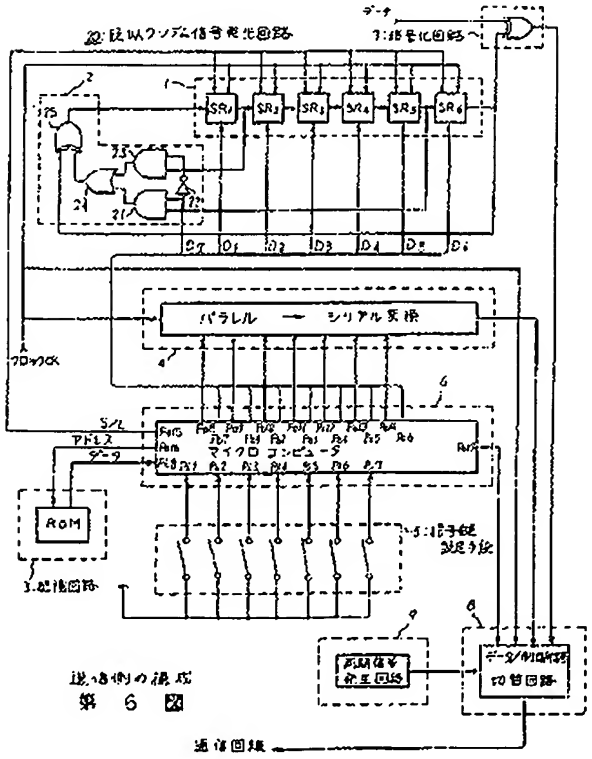
第 2 図



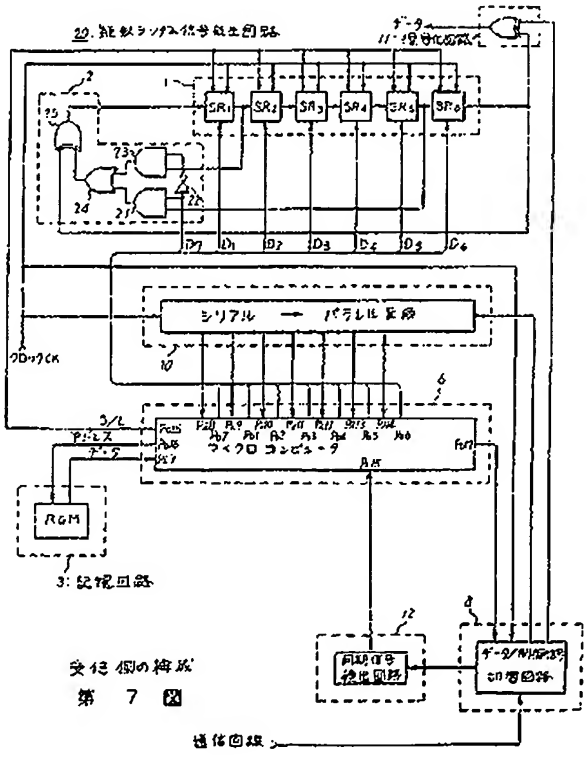
第 3 図



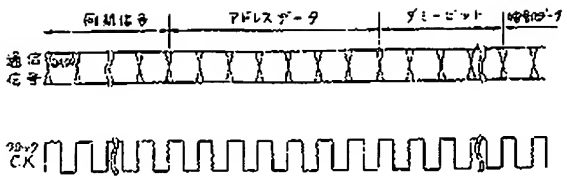
第 4 図



送信側の構成
第 6 図

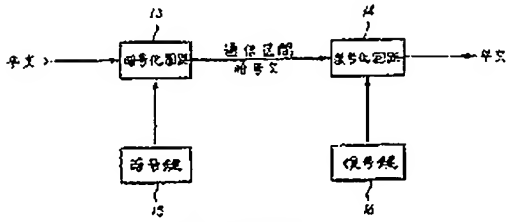


受信側の構成
第 7 図




通信信号の一例

第 8 図




従来例の構成図

第 9 図